UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,848	12/21/2001	Ynjiun P. Wang	Wang P007	1158

7590 05/24/2005

MOSER, PATTERSON & SHERIDAN, LLP
350 CAMBRIDGE AVENUE, SUITE 250
Palo Alto,, CA 94306

EXAMINER	
CHEUNG, MARY DA ZHI WANG	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/026,848	WANG, YNJIUN P.	
	Examiner	Art Unit	
	Mary Cheung	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) *1-4 and 9* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-8 and 10-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of the Claims

1. This action is in response to the amendment filed on March 17, 2005. Claims 1-17 are pending. Claims 1-4 and 9 are not elected and are withdrawn from consideration. Claim 5 is amended. Claims 5-8 and 10-17 are elected and examined.

Response to Arguments

2. Applicant's arguments filed March 17, 2005 have been fully considered but they are not persuasive.

In response to applicant's argument that Dorenbos (U. S. Patent 5,751,813) fails to teach the server does not encrypt or decrypt the message as claimed in claim 5, examiner respectfully disagrees. Dorenbos teaches the first-stage encrypted message 105A (see Fig. 2) remains encrypted in the server (column 3 lines 27-48 and Fig. 2).

In response to applicant's argument that Dorenbos fails to teach derive share secret, examiner believes that this matter is taught by Dorenbos as generating an digital data message that is to be shared with designated recipient (column 3 lines 5 – column 4 line 10 and Fig. 2).

Regarding applicant's arguments that the methods are taught by the cited prior art are not as secure as the teaching presented in the current application, examiner believes that the differences are not explicitly shown in the applicant's claims, and the cited prior art clearly match the claimed language.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 5-8 and 10-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Dorenbos, U. S. Patent 5,751,813.

As to claim 5, Dorenbos teaches a method of exchanging secured messages between first and second registered PEAD users over the internet and a server utilizing at least one PEAD, comprising the steps of (column 3 line 1 – column 4 line 3 and Fig. 1; *specifically, the PEAD corresponds to items 103, 111, 115, 119, 121, 127 and 131 of Fig. 1*):

a) obtaining public key information using a receiving PEAD user's ID as an index (column 4 lines 23-25, 53-60);

b) electronically deriving a shared secret using a receiver's public key (column 3 lines 4-18 and Fig. 2; *specifically, the shared secret corresponds to the generated digital message as described in column 3 lines 5-6 of Dorenbos' teaching*);

c) a sending PEAD user then electronically encrypting a message with the shared secret and sending it with the receiver's user ID appended with the user's ID (column 3 lines 4-26 and Fig. 2);

d) then the receiving PEAD user using the sender's user ID and sender's public key information to derive the shared secret, the message remaining encrypted while handled by the server (column 3 lines 27-48 and column 4 lines 4-10 and Fig. 2; *specifically, "the message" corresponds to the first-stage encrypted message in Dorenbos' teaching*).

As to claim 6, Dorenbos teaches storing one or more of the other PEAD users' share secret using the sender's ID as an index (column 3 lines 4-15 and Fig. 2).

As to claim 7, Dorenbos teaches the sender retrieves the public key information using the receiver's user ID from the server (column 3 lines 12-18 and column 4 lines 23-25 and Fig. 2).

As to claim 8, Dorenbos teaches after the sender encrypts the message with the shared secret, sending it to the server with the receiver's ID appended (column 3 lines 12-25 and Fig. 2).

As to claims 10-11, forwarding the message when the receiver's PEAD is polling for messages, and the server pushing the message to the receiver's PEAD are taught by Dorenbos as transmitting the message to the receiver's PEAD (column 3 lines 36-48).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos, U. S. Patent 5,751,813 in view of Spies et al., U. S. Patent 6,055,314.

As to claim 12, Dorenbos teaches the sender's public key is stored on a server and is indexed by the sender's ID (column 4 lines 23-25). Dorenbos does not specifically teach the sender causing the PEAD to generate a key pair comprising a public key and a private key, and then transferring the public key to a server. However, Spies teaches sender causing a portable electronic device to download cryptographic keys, and then transferring the keys to a server (column 6 lines 56 – column 7 lines 3 and column 7 lines 55-67 and Fig. 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the teaching of Dorenbos to include the feature of having the PEAD generate a key pair and then transferring the public key to a server so that the PEAD would be able to easily and quickly obtain the cryptographic keys for using them to securely transmitting messages.

7. Claims 13-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos, U. S. Patent 5,751,813 in view of Blakley, III et al., U. S. Patent 5,677,952.

As to claim 13, Dorenbos teaches exchanging secured messages between first and second registered PEAD user as discussed above. Dorenbos does not specifically

teach the receiver checking for a stored shared secret in a shared secret table of the PEAD, and after finding the shared secret using the shared secret to decrypt the senders message. However, this matter is taught by Blakley as the secret is stored in a table (abstract and column 6 line 20-40 and Fig. 3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow Dorenbos' teaching to include a table that comprises the shared secret for efficient organizing and fast retrieval of the shared secret.

As to claim 14, if the receiver does not find a shared secret in the shared table then the receiver retrieves the sender's public key information from the server using a sender's user ID as an index is taught by Dorenbos as retrieves the sender's public key information from the server using a sender's user ID as an index (column 4 line 11 – column 5 line 13).

As to claim 15, Dorenbos teaches the receiver using the receiver's private key and the now-retrieved sender's public key to compute the shared secret (Figs. 2-4).

As to claim 16, Dorenbos teaches storing the shared secret, using the senders ID as an index (column 3 lines 12-36 and column 4 lines 23-25).

As to claim 17, Dorenbos modified by Blakley teaches the shared secret stored in the shared secret table as discussed above. Dorenbos modified by Blakley does not specifically teach periodically updating the shared secret. However, it would have been obvious to one of ordinary skill in the art to allow the teaching of Dorenbos modified by Blakley to include periodically updating the shared secret for efficiently organizing the most updated information.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is 571-272-6705. The examiner can normally be reached on M-Th (10:00-7:30) Second Friday Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mary Cheung
Patent Examiner
Art Unit 3621
May 20, 2005

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600